Course 5 Week 3

FORENSIC

What is Forensics?

Digital Forensics, is a application of sciene to the identification, collection, examination, and analysis of data while preserving the integrity to the information. and maintaining a strict chain of custody for the data.

Types of data

1.) CD/DVDs

2.) Internal & External Drives

3.) Volatile Data

4.) Network Activity.

5.) Application Usage

5.) Application Usage

6.) Portable Digital Devices.

The need for forensics.

→ Criminal Investigation

→ Incident Handling

→ Operational Troubleshooting

→ Log Monitoring

→ Data Recovery

→ Data Acquisition

→ Due Diligence / Regulatory

Compliance.

Forensic Process

- Collection
- Examination
- Analysis
- Reporting

The Forensic Process.

→ Data Collection & Examination.

→ Externally owned Property

→ Computers at Home OFFICE

→ Alternate sources of Data

→ Logs

→ Keystroke Monitoring.

Steps to Collect Data

→ Develop a plan to aspire the data
→ Aquire the Data
→ Verify the integrity of the data.

Examination
→ By Passing Controls
→ A sea of Data
→ Tools.

Analysis → putting the pieces together.

Famous Case solved using Digital Forensic

1.) The BTK Killer Dennis Rader.
→ A floppy Disk Nectar Sent to Police revealed his true identity

2.) Dr. Conard Murray's lethal prescription.

Investigations discovered documentation on Dr. Murray's computer showing his authorization of lethal amounts of the drugs.

3.) The Craiglist, Philip Markoff.

Investigators tracked the IP address from the emails used in the Craiglist correspondence.

Reporting.

Report Composition.

1.) Overview/Case Summary.

2.) Forensic Acquisition & Examination Preparation

3) Findings & Report

4) Conclusion

Forensic Data.

File Systems.

Windows	Unix	macOS
FAT	· EXT	HFS+
12	2	APFS
16	3	
32	4	
NTFS	Reiser FS	
ReFs	XFS	
	ZFS	
	Btrfs.	

What's not there.

Deleted files → When deleted it doesn't disappear. It is just seen as deleted.

Slack space → space is allocated as-is regardless of small file size

Free space → not allocated to any partition.

MAC Data.

Modification, Access and Creation time data.

Logical Backup.

↳ Copies the directories and files of a logical volume. It does not capture other data that may be present on the media, such as deleted files or residual data stored in slack space.

(can be used on Live go
if using a standard backup software

Imaging:

Generates a bit-for-bit copy of the original media, including free space and slack space.

Tools For Techniques:

1.) File Viewers
2.) Uncompressing Files
3.) GUI for Data structures
4.) Identifying Known Files
5.) String Searches & Pattern Match
6.) MetaData

Recovering System Data:

Volatile

Slack space

Free space

Network Configuration & connecting

open Files

Running Processes

Login Sessions

Operating System Time

Non-Volatile

Configuration Files

Logs

Application Files

Data Files

Swap Files

Dump Files

Hibernation File

Temporary Files.

Application Data.

Config settings -> Configuration File

Runtime Options

Access to source code

Authentication → External Authentication
Proprietary Authentica

Pass-through Authentication

Host/User Environme

Logs → Event
Audit
Error
Installation
Debugging.

Data →
Supporting Files → Documentation
Links

Graphics.

All Architecture → Local
Client/Server
Peer-to-Peer.

Web Data From Host

→ Favorite Web sites
→ History w/ time stamps of website visit
→ Cached web data files
→ Cookies.

Web Data from server.

→ Timestamps
→ IP address
→ Web Browser Version
→ Type of Request.

→ Resource Requester.

Collecting Application data

File system → Volatile OS Data → Network Traffic.

Network Data.

TCP/IP

Application Layer → This layer sends and recieves data for particular applications, such as Domain name system (DNS). Hypertext Transfer Protocol, (HTTP) Simple Mail Transfer Protocol (SNMP).

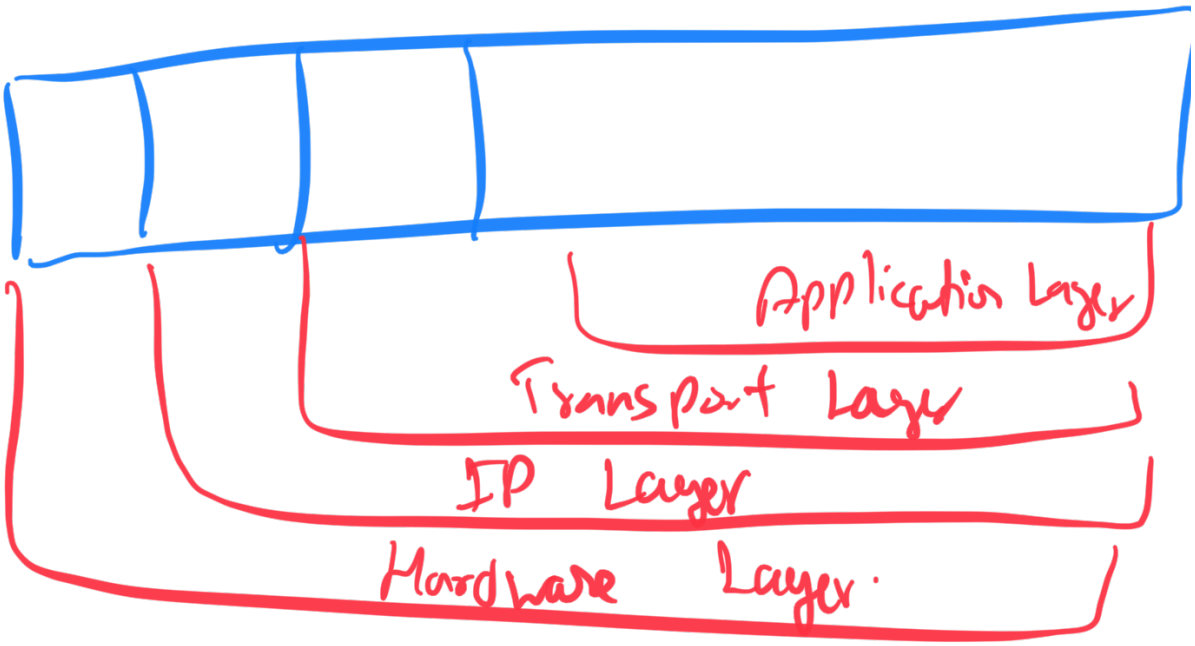
Transport Layer → Provides Connection-oriented or connectionless services for

transporting application layer services between networks. The transport layer can optionally ensure the reliability of communication. TCP, UDP are commonly used transport layer protocols.

Internet Protocol Layer (network layer)
This layer routes packets across networks. IP is the fundamental network layer protocol for TCP/IP. Other commonly used protocols at the network layer are Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP).

Hardware Layer (Data Link Layer)
This layer handles

Communication on the physical network components. The best known data link layer protocol is Ethernet.



Sources of Network Data.

- Firewalls — Packet Sniffers & Protocol Analyzers → IDS
- Security Event Management software. — Network Forensic Analysis Tools ← Remote Access